

INTERCONNECTED AND INTERDEPENDENT: *VULNERABILITIES BEYOND Y2K*

The information technology revolution sparked the globalization of the world economy and marched the world into the information age. But revolutions often usher in unintended consequences. The Y2K problem is one of the unintended consequences of the information age.

Since its formation, the Committee has investigated the Y2K-readiness of individual critical infrastructures. Infrastructures are the framework and systems that provide a reliable flow of products and services essential to the defense and economic security of the U.S., the smooth functioning of government at all levels, and society as a whole.¹

To understand the broad Y2K challenges facing the nation's commerce and defense, the Committee implemented a horizontal approach to identify key interdependencies across infrastructures. In its investigations, the Committee learned that the Y2K problem is a complicating factor in an already challenging information technology landscape. If complex information systems can easily be disrupted by accident or something as innocuous as the Y2K computer problem, what dangers are

posed by those seeking to exploit system vulnerabilities? While the interconnectedness of systems increases efficiency, it also heightens vulnerability.

The globalization of the world economy and the integration of markets, nation-states, and technologies "is enabling individuals, corporations, and nation-states to reach around the world farther, faster, deeper, and cheaper than ever before."² Cheap global reach, however, exacts unexpected costs from the nation's critical infrastructures, economy, and defense.

**"THE THING WE HAVE
LEARNED OUT OF Y2K IS IN
ADDITION TO THE
TREMENDOUS PRODUCTIVITY
WE GET OUT OF COMPUTERS,
THERE IS A VULNERABILITY
THAT WILL BE WITH US."**

--SENATOR BENNETT

UNDERSTANDING VULNERABILITIES

What is information warfare or cyber warfare? According to experts, adversaries can exploit the tools and techniques of the information revolution to create large-scale or serious disruptions in key national infrastructure sectors.³ Disrupting the networks that drive such sectors as energy, telecommunications, transportation, and finance could have a profound effect on our nation's defense and economy. "Our modern electronic infrastructure—computer systems that control everything from

our power systems to our stock exchanges—is a potential target for attack by computer hackers and organized criminal enterprises. Such attacks pose a direct threat to our national security.”⁴ The tools required to attack automated systems are relatively inexpensive and readily available. Furthermore, the expertise in how to target, identify, and compromise systems is readily available on the Internet. According to Interpol, the European police agency, the Internet has some 30,000 hacker-oriented Web sites, and roughly 17 million people have the necessary computer skills to do damage.⁵

**...THE INTERNET HAS BEEN
TURNED INTO A KIND OF
WEAPON FOR WARFARE
SO, AMERICA’S ENEMIES ARE
ABLE TO INFLICT
IRREPARABLE LOSSES ON THE
U.S. ARMY THROUGH USE OF
THE INTERNET.”**

**--IRANIAN MILITARY
JOURNAL**

- foreign intelligence services;
- rogue nations;
- organized crime;
- corporate espionage;
- terrorists;
- disgruntled employees/trusted insiders; and
- casual techno-thrill seekers.

Each of these sources can inflict serious damage on public or private systems. The technology to cause such damage is increasingly sophisticated and the skills required to operate it are declining. In short, it is getting easier for an adversary to compromise an unprepared system.

So how bad is it? The real threat of intrusion is difficult to assess. Intrusion incidents are hard to detect and often go unrecognized; failures or disruptions resulting from intrusion activities are frequently attributed to operator or user error; threat incidents are not always documented for further study or investigation; and, even when attacks are identified as incidents, they often go unreported.⁶

Cyber-intruders can attack from “virtually” anywhere, disguising locations and leaping through international gateways, making identification and attribution extremely difficult. Determining the source and the intention of an attack is an arduous task because the broad threat spectrum includes:

Those engaged in organized crime and corporate espionage generally want to quietly insert themselves for financial gain and are usually not interested in destroying a particular system. Disgruntled employees, terrorists, and rogue nations, however, could be seeking only highly visible, highly destructive targets. Foreign intelligence services present a more complex threat. The information they collect can allow them to erode a nation’s defense technologies or key commercial sectors. At the same time, the systems they exploit create a roadmap for a possible attack. It is not impossible for these players to meet in cyberspace and unknowingly use one another to accomplish mutually beneficial goals. Techno-thrill seekers, often the stereotypical teenage hacker, can compro-

mise national security, destroy, and cause problems without a specific agenda or motive. But a more serious and enduring concern than techno-thrill seekers and hackers should be those who would conspire to engage in information warfare.

Opportunity, Access, and Skill

The unprecedented scope of Y2K corrections over the past several years, and the lack of accountability for whom did what to which piece of software or hardware, is an unsettling confluence of opportunity, access, and skill. Existing vulnerabilities and the increasing interest of foreign countries to exploit these vulnerabilities have concerned the intelligence community for several years. As the Committee noted in its last report, the President's Commission on Critical Infrastructure Protection (PCCIP) recognized the potential for the Y2K problem to create long-term concerns in the infrastructures. Late starts have compelled many organizations to contract-out work on sensitive systems. In some cases, organizations are sending code overseas to foreign firms. This gives potentially unscrupulous programmers the opportunity to tamper with code. The PCCIP further cautioned that the broad scope of Y2K corrections could allow an adversary to build an exceptional understanding of sensitive systems, thus enabling it to "design a subtle or comprehensive attack" against critical systems.⁷

Between 1995 and 2000, a significant amount of the nation's software will have been reviewed and remediated, often overseas. The effort to fix the code may well introduce serious long-term risks to the nation's security and information superiority. Some risks are introduced by accident and some are maliciously placed, but both could erode U.S. national security and emergency preparedness if left unchecked.

While unintended errors can create problems, intentionally malicious coding problems can be far more hazardous. Key risks include:

➤ **Trap doors that allow**

- intruders to gain anonymous access
- root access of network
- access to proprietary and sensitive information

➤ **Malicious code that**

- can destroy hardware/software
- can deny and disrupt access
- may take the form of logic bombs
- may include Trojan horses and,

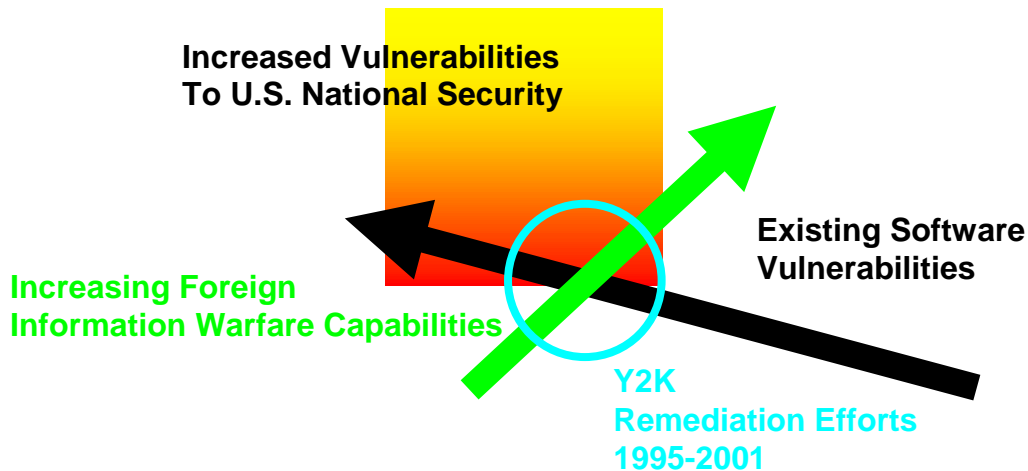
➤ **Long-term consequences may include**

- increased foreign intelligence collection
- increased espionage activity
- reduced information assurance
- a loss of economic advantage
- an increase in key infrastructure vulnerability

INVESTIGATING THE YEAR 2000 PROBLEM: THE 100 DAY REPORT

There is currently no automated way to scan for malicious code or trapdoors. Why is this a problem? A trap door can take as little as four lines of code, and a typical phone switch can have several millions lines of code. The odds of catching this code are

cious code. The desire for easy-to-use open systems has resulted in systems that are user-friendly, but extremely difficult to administer and configure for secure use. Security features are frequently viewed by software developers as a hindrance



not good. If a trap door is inserted into key network software, an adversary could gain access for years without anyone being the wiser. It is this long-term unnoticeable access that enables key information to be lifted without a trace. This is information that could enable adversaries to target key infrastructure systems and capture important research and development technologies for economic advantage. We face a dangerous intersection of rapidly-developing foreign information warfare (IW) capabilities and the amount of code that has been remediated in countries with known IW interests.

The increasing complexity of today's software makes it difficult, if not impossible, to identify potential vulnerabilities and to discover mali-

with little market value and are often ignored. The software development community has generally failed to apply the lessons learned from intrusion attacks when developing new software and, as a result, new software is issued with the same vulnerabilities as the prior version.⁸

SO WHAT HAPPENS WHEN YOU PUT Y2K INTO THE MIX?

U.S. adversaries could find it easier to exploit the U.S., capitalizing on Y2K software corrections. In the scramble to correct Y2K problems it has become advantageous and even necessary to contract-out remediation efforts. Organizations both private and public bring in temporary contractors and employ com-

INVESTIGATING THE YEAR 2000 PROBLEM: THE 100 DAY REPORT

mercial-off-the-shelf based software tools for remediation. The end result is this: foreign nationals without background checks are given extensive access, influence and control of software. Many of the countries involved in Y2K remediation are actively pursuing IW capabilities and their respective intelligence agencies are closely tied with their economic sectors. According to press reports, security firms have already found "trap doors" in Y2K remediation. Some were placed to provide reputable firms an entry for future repairs, but others have been intentionally hidden. One incident involved a major information technology company that used a Pakistani company that has since gone out of business.⁹ This juxtaposition of opportunity and access present a credible risk to the national security of the U.S.

In addition to software-specific information, contractors gain insight into the entire organization's infor-

mation enterprise. Y2K program offices have succeeded in consolidating the inventories and assessments of an organization's information assets. Programmatically, this has been helpful. However, Committee interviews have found time and again that security has taken a back seat to deadlines.

This access and control could evolve into long-term security and cyber-vulnerabilities. The Gartner Group has already projected a "one billion dollar Y2K heist."¹⁰ If Y2K security compromises prompt people to steal money electronically, rest assured that there will be more nefarious attempts to steal ideas of much greater value.

Aside from traditional counterintelligence concerns, Y2K-related backdoor access could be exploited for fraud, theft, industrial espionage, and/or disruptions. Programmers contracted to fix the Y2K bug will use their access to leave a "backdoor," granting them the ability to come and go undetected. Furthermore, the comprehensive inventory and assessments of IT systems have given many contractors and "outsiders" a comprehensive roadmap to organizations critical systems and core processes, both in the federal government and in the private sector. Unfortunately, these broad security risks translate into long-term infrastructure vulnerabilities and present unique challenges to national security. The U.S. might find itself more vulnerable to information warfare attacks--not just on January 1, 2000,

Foreign Countries Involved in Industrial Espionage, Offensive Information Warfare Initiatives, and U.S. Y2K Remediation			
Country	Economic Espionage	Offensive Information Warfare Initiative	Major U.S. Y2K Remediation Provider
Bulgaria	YES*	Limited	
China	YES*	YES	YES
Cuba	YES*	LIMITED	
France	YES*	YES	
India	YES*	YES	YES
Iraq	YES*	YES	
Ireland			YES
Israel	YES*	LIKELY	YES
Japan	YES*	LIKELY	
Pakistan			YES
Philippines			YES
Russia	YES*	YES	
South Korea	YES*	YES	
Countries identified by the National Communications System as using electronic intrusions, usually for industrial espionage purposes, ¹			

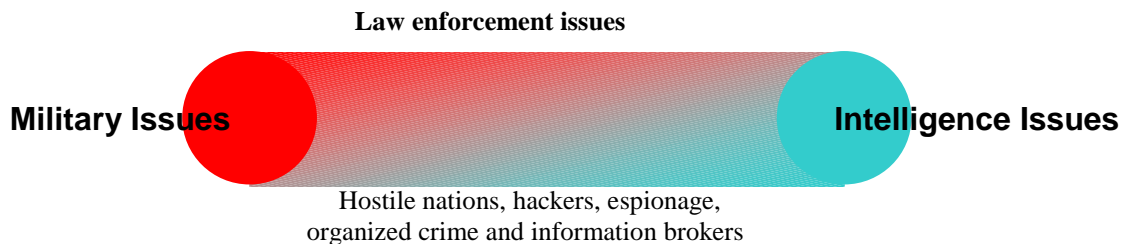
but also for sometime into the future.

PROTECTING CRITICAL INFRASTRUCTURE

Traditionally, the U.S. has viewed national security threats as physical. We have maintained confidence in our ability to field and maintain the

ports, the most lucrative information obtained includes research and development strategies, manufacturing and marketing plans, and customer lists.¹³

The information security risk spectrum range can be grouped into 3 broad categories: military/national security, law enforcement, and intel-



best defenses and military in the world. But what if the threat is not coming from a bomb, a submarine, or a show of force? Although the effect of an electronic attack on a telecommunications or information system is not as dramatic as the physical impact of a bomb, the results can be far more destructive to a modern society.¹¹ Furthermore, adversaries can exploit technology to conduct operations from another country or from multiple locations.

The government is not always the primary target. Increasingly, it is the private sector that is being attacked. According to the National Counterintelligence Center (NACIC), the governments of at least 23 countries are targeting U.S. firms.¹² Targets regularly include high-tech companies, manufacturing, and service industries. According to press re-

ligence. Unfortunately, the law enforcement portion of the equation is the most challenging. Because it is often virtually impossible to detect the source or motivation of a security violation, the U.S. currently has no precise response mechanism. The asymmetrical nature of the information-based threats further complicates the response and decision making process.

President Clinton signed Presidential Decision Directive 63 (PDD 63) in May 1998. PDD 63 required the Executive Branch to assess the vulnerabilities of its computer-based systems and to remedy deficiencies in order to become a model of information security. Under PDD 63, the federal government is called upon to produce a detailed plan to protect U.S. critical infrastructure and to defend America against information

warfare. The PDD was a giant step forward in recognizing the new vulnerabilities facing the U.S. Despite progress with the PDD, four key elements necessary for a successful infrastructure protection strategy must still be addressed.¹⁴

First, the PDD does not set up a process to identify what is critical. Without such a process, national planners will have no basis upon which to make decisions on committing scarce resources. The absence of clear priorities has complicated the creation of the National Plan, which was due in the fall of 1998. In the process of addressing the Y2K problem, the U.S. government and the private sector have both had to carefully scrutinize their core mission and the thin line systems that support their operations. This identification represents a fleeting national resource. Examining the critical interdependencies of assets both in government and in industry might allow the U.S. to finally define a minimum essential information infrastructure. The national Y2K effort has made a unique and unexpected contribution to the critical infrastructure protection effort. Y2K has forced every government agency, key economic sector, and state and local entity and organization to identify and define what is critical. Never before have government and industry had such clarity about their respective mission-critical systems. Now is the time to define a response, recovery, and reconstitution ability to ensure the integrity of these systems.

Second, the PDD does not address the information warfare threat. It focuses a great deal on criminal hackers and terrorists, but not at all on the emerging information warfare threats posed by foreign nations. From the standpoint of national strategy, there is a big difference between protecting against individual hackers and protecting the nation against a systemic attack. According to the General Accounting Office, "Official estimates show that more than 120 countries already have or are developing such computer attack capabilities."¹⁵ Russia, China, South Korea, Cuba, India and Iran have all shown interest in such capabilities.¹⁶ China, for example, recently called for the creation of a special hacking force composed of military and civilian specialist who could engage in internet warfare¹⁷ A state-sponsored or coordinated event could challenge all of our existing response and coordination capabilities. Experts contend that, with available tools on the Internet and a modest investment in technology, a coordinated debilitating cyber-attack on key U.S. systems is possible. The severity of the attack could exponentially escalate with the right sponsorship.

Third, the PDD does not identify the elements of a defense against information warfare attack, nor does it assign responsibility for such defenses. The Defense Department (DOD) is actually assigned very few duties. Recently the DOD created a Joint Task Force on Network Defense (JTF-CND). One of its main daily tasks is to coordinate across DOD (commands and services) to help stop computer attacks,

contain damage, and restore functionality. But JTF-CND is only responsible for the DOD. Who defends the rest of the government? Who defends private industry? Industry can certainly protect itself from annoying hackers and possibly even some espionage, but if it finds itself swept into a sophisticated IW attack, who is responsible?

Fourth, the PDD does not establish an indications and warning architecture that would discern preparations for an information attack; nor does it set up a system that would detect if and when national systems were under attack. In many ways, the Y2K event creates an opportunity to understand and define the necessary thresholds needed to establish such an architecture. There is a brief opportunity to benefit from the intellectual capital and expertise that may evolve at the Information Coordination Center and the DOD's Decision Support Activity.

How do you defend against a threat that is not necessarily military? What happens when you can't determine who the adversary is? Who responds: law enforcement or defense? What happens when civilian infrastructure and private industry are the targets? At what point does an action cease being a law enforcement issue and start becoming a national security threat? Right now there are no easy answers to these questions.

Meanwhile, cyber attacks continue. Currently, the DOD suffers from an intensive and dangerous series of sustained intrusions code named

Moonlight Maze. Essentially, Moonlight Maze is a wholesale attempt to mine sensitive information from the U.S. The Intruders, who are believed to be Russian, conduct their collection efforts by hiding in the twisted labyrinth of cyberspace. Operating out of the Russian Academy of Sciences, the hackers are believed by some in the Pentagon to be "a state sponsored Russian intelligence effort."¹⁸ The perpetrators of Moonlight Maze have locked onto America's soft digital underbelly exploiting both policy and technological vulnerabilities. The Committee believes that is only the beginning of things to come.

Currently the DOD and the National Infrastructure Protection Center (NIPC), housed at the Federal Bureau of Investigation, are working together to remedy Moonlight Maze crisis. But investigation and solutions don't seem to be keeping pace.

According to a former head of Soviet counterintelligence, Oleg Kalugin, the Federal Agency for Government Communications and Information (a former KGB unit specializing in electronic eavesdropping) was certain to be exploiting the Internet for spying on America.¹⁹

Russia's financial troubles have prompted painful cutbacks in military research funding. High-tech industries and military research and development become attractive and electronically accessible targets. "*Russia is quite good at producing technology but can't afford to finance the research,*" said Kalugin. "*It's easier to steal it.*"²⁰

Right now cyber-intruders may be just collecting information, but they could exploit this information to disrupt key national programs and infrastructures. In a recent Iranian military journal the author observed, “...the Internet has been turned into a kind of weapon for warfare managed by information technology. Indeed the Internet is linked to all important information centers, including 150,000 computers belonging to the US Army. So, America’s enemies are able to inflict irreparable losses on the US Army through use of the Internet.”²¹ The DOD can’t protect against a threat of such unprecedented scope.

In a limited fashion, Y2K provides a nationwide test bed for dealing with what the effects of a deliberate attack on the information infrastructure might look like. It is an excellent opportunity for the U.S. to learn what is needed to coordinate and reconstitute from a potential information warfare event. But the U.S. response will be closely monitored by foreign intelligence looking for organizational weaknesses and policy oversights that could be exploited in the future. Y2K is an opportunity to educate ourselves first hand about the nature of 21st century threats and challenges.

WHERE DO WE GO FROM HERE?

Regardless of the intentions and motivation behind a cyber-attack—whether espionage, pollution of data, manipulation/control of a system, or mere destruction—there is a broad

continuum of means employed. This continuum ranges from the use of a person employed or inserted to do the deed from the inside, through the surreptitious introduction of doctored software enabling an exterior attack, to hacking through fire walls from the outside. Given this broad spectrum of means employed in cyber-attack, and the very wide range of targets and purposes, this issue far transcends the narrow scope of defense, law enforcement, or intelligence.

Protecting America’s critical infrastructures is more than finding a balance between firewalls and firepower. There are serious and sometimes contentious policy issues that will need to be resolved in both the legislative and executive branches. These issues will challenge the Congress to work across many different jurisdictional boundaries.

Currently there is no common understanding of what constitutes a “nationally significant” cyber-incident. A qualitative framework needs to be developed which takes into account that several incidents in “seemingly” unrelated sectors may well be coordinated and purposeful attacks. A well-defined threshold must take into account both low intensity incidents in multiple sectors as well as widespread disruption of a single infrastructure.

Furthermore, there is a need to understand of what are the minimum essential infrastructure (MEI) requirements for maintaining U.S. national security and emergency preparedness. An operationally

INVESTIGATING THE YEAR 2000 PROBLEM: THE 100 DAY REPORT

significant understanding of MEI must also consider the criticality of key regions and communities within the U.S. It is important to understand that these may be communities that are not just vital to defense and force projection. Indeed they may well be commercial centers critical to communications, information technology, energy and manufacturing.

Understanding interdependency is essential to successfully articulating thresholds and MEI. But this is no easy task and will involve both government and industry collaborations and industry to industry collaborations. If we are to move into the next century maintaining U.S. sanctuary, then we must realize that national security is a shared responsibility. The threat of IW is bigger than defense, justice and intelligence and the federal government. Protecting against information based threats means working with state and local governments as well as international partners.

Finally there are legal and regulatory issues which will need to be investigated and considered in the context of asymmetrical threats. The Post Cold War environment makes the security of the U.S. much bigger than DOD. Eliminating infrastructure vulnerabilities and determining how to facilitate reconstitution will require the examination of existing laws. As we learned in the Y2K experience, information sharing is essential. However, sustained information sharing raises many questions about liability, antitrust and law enforcement. Liability and antitrust fears

may be impediments for owners and operators of critical infrastructures to exchange information.

Protecting the U.S. from 21st Century threats will require a new level of cooperation between law enforcement, the national security and intelligence communities²², civil departments and agencies, lawmakers and the judiciary. Congress will need to investigate and ensure that the standing legislation defining the concepts of national security and foreign intelligence are robust enough to deal with the cyber warfare, new technologies and asymmetrical threats.

Finally, as we have learned in addressing Y2K we have to understand that many critical infrastructures do not end at the U.S. borders. Telecommunications, energy, banking and finance, and transportation are global infrastructures whose disruption has direct and indirect consequences on our nation's commerce and defense. Key U.S. infrastructures have assumed a global character. We need to consider how the new geography of globalization is impacting international law and agreements. It is important to understand the complexities created by the absence of an international legal framework for cyber-crime. In some countries cyber attacks or intrusions are not considered crimes and there is often little cooperation with U.S. law enforcement. In many cases such as the Israeli Hacker, who masterminded intrusion into DOD systems, countries refuse to extradite the criminals.²³

INVESTIGATING THE YEAR 2000 PROBLEM: THE 100 DAY REPORT

Government can't solve this entire problem, but it can coordinate and facilitate reconstitution and recovery. Right now the Administration does not even have a definition of cyber-reconstitution. Congress must become active and investigate ways to focus research and develop initiatives that will enable the U.S. to organize warning, damage assessments, and coordination of cyber-reconstitution.

We are interconnected, interdependent and vulnerable. We also can't go

back. Rather, we must examine the technological topography of the nation with an eye on the future. We must have an appropriate policy framework to ensure that infrastructure protection concerns are factored in to related national policy decisions, such as regulatory reform and encryption legislation. Finally, we need the determination and vision to ensure the integration of the fundamental American ideals of liberty, freedom, and justice into the bits and bytes that pave the information superhighway.

¹ Critical Foundations: Protecting America's Critical Infrastructures (PCCIP report, October 1997). www.pccip.gov

² Thomas L. Friedman The Lexus and the Olive Tree, Farrar Straus and Gruax, New York 1999. Pg. 7

³ Roger C. Molander, Peter A. Wilson et al Strategic Information Warfare Rising, RAND 1998 <http://www.rand.org/publications/MR/MR964/index.html>

⁴ International Crime Control Strategy of the United States, Section VII: Responding to Emerging International

CrimeThreats, <http://www.usdoj.gov/criminal/press/VIIIresp.html>, May 12, 1998.

⁵ "War.com" Frank Vizard Popular Science Thursday, July 1, 1999 Volume 255, Issue 1

⁶ PCCIP, *Critical Foundations: Protecting America's Infrastructure*, Washington, DC: USGPO, October 1997, pp. 14-18.

⁷ Critical Foundations: Protecting America's Critical Infrastructures (PCCIP report, October 1997). www.pccip.gov

⁸ The Electronic Intrusion Threat to National Security and Emergency Preparedness (NS/EP) Telecommunications: An Awareness Document. The National Communications System March 1999.

⁹ "\$1 billion Y2K heist predicted Upgrades leave systems vulnerable" M.J. Zuckerman, USA Today. Friday, July 16, 1999.

¹⁰ "\$1 billion Y2K heist predicted Upgrades leave systems vulnerable" M.J. Zuckerman, USA Today. Friday, July 16, 1999.

¹¹ The Electronic Intrusion Threat to National Security and Emergency Preparedness (NS/EP) Telecommunications: An Awareness Document. The National Communications System March 1999.

¹² National Counterintelligence Center (NACIC), *Annual Report to Congress on Foreign Economic Collection*

INVESTIGATING THE YEAR 2000 PROBLEM: THE 100 DAY REPORT

and *Industrial Espionage*, Washington, DC: USGPO, October 1997, p. 18.

¹³ Jack Nelson, "U.S. Firms" 97 Losses to Spies Put at \$300 Billion," *Los Angeles Times*, January 12, 1998.

¹⁴ Crime, Terror and National Security in the Information Age. The Senate Judiciary Subcommittee on Technology, Terrorism and Government Information, November 1998.

¹⁵ Information Security: Computer Attacks at Department of Defense Pose Increasing Risks (Chapter Report, 05/22/96, GAO/AIMD-96-84).

¹⁶ Japan, France, Germany, Israel, Bulgaria, Ireland, Pakistan and others

¹⁷ "Chinese Military Calls for Special Hacker Force" Newsbytes August 4, 1999.
(<http://asia.yahoo.com/headlines/050899/technology/933807180-134396.html>)

¹⁸ Gregory Vistica "We're in the Middle of a Cyber war" Newsweek September 13, 1999
http://newsweek.com/nwsrv/printed/us/st/sr0612_5.htm

¹⁹ Matthew Campbell "Russian hackers steal US weapons secrets" Sunday Times – London Times Newspapers Ltd, Sunday, July 25, 1999

²⁰ Matthew Campbell "Russian hackers steal US weapons secrets" Sunday Times – London Times Newspapers Ltd, Sunday, July 25, 1999

²¹ "Electronics to Determine the Fate of Wars" *Nashriyeh-Esias Nezami* December 22, 1998, Translated in FBIS FTS 199902001199

²² The U.S. intelligence community, includes the Central Intelligence Agency, the National Security Agency, the Defense Intelligence Agency, the intelligence agencies of the different services and the Federal Bureau of Investigation

²³ In the Spring of 1998, Defense Department networks experienced one of their most widespread and systematic attacks to date. The attacks occurred while the military was trying to deploy forces to the Persian Gulf in response to Iraqi provocations. For over 4 days, the defense community and law enforcement agencies struggled to understand the nature of the attacks and identify the threat. The attacks were launched from computers within the United States and overseas. As it turned out, this incident involved a couple of California teenagers who were being tutored by an Israeli hacker. The Israeli hacker was later recruited by the Israeli Army and was not available for prosecution in the U.S.